

UNITED STATES OF AMERICA  
CYBERSPACE  
SOLARIUM  
COMMISSION

Background, Emerging Strategy, and Recommendations

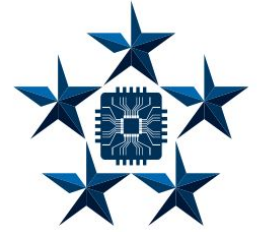
*November 2020*

# Agenda



1. **What is the Commission?**
2. **Content of:**
  - a. **Commission Report and**
  - b. **White Papers**
3. **Status**
  - a. **What happened in 2020?**
  - b. **What's the plan for 2021?**
4. **What this means for Resilience and Engaging the Private Sector**

# The U.S. Cyberspace Solarium Commission



Bipartisan, intergovernmental body created by the 2019 NDAA to develop a strategic approach to defending the United States in cyberspace against cyberattacks of significant consequence.

CSC draws inspiration from its namesake, the “Solarium Project” convened by President Eisenhower in 1953.



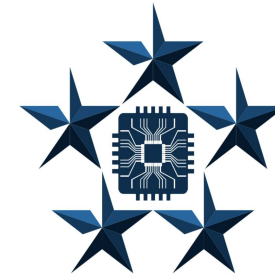
## STATUS UPDATE

400+

STAFF  
ENGAGEMENTS

30 +

COMMISSION  
MEETINGS



UNITED STATES OF AMERICA  
CYBERSPACE  
SOLARIUM  
COMMISSION

## MANDATE

Section 1652 of the Fiscal Year 2019 National Defense Authorization Act (NDAA) established the Cyberspace Solarium Commission as an independent Commission to “develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences.”

## COMMISSIONERS

4

### LEGISLATIVE BRANCH



**Sen. Angus King**  
I-ME  
(Co-Chair)



**Rep. Michael Gallagher**  
R-WI  
(Co-Chair)



**Sen. Ben Sasse**  
R-NE



**Rep. Jim Langevin**  
D-RI

4

### EXECUTIVE BRANCH



**Andrew Hallman**  
Fmr. ODNI



**David Norquist**  
DOD



**David Pekoske**  
DHS



**Chris Wray**  
FBI

6

### ACADEMIA, THINK TANKS, PRIVATE SECTOR



**Frank Cilluffo**  
Auburn University



**Chris Inglis**  
U.S. Naval Academy



**Suzanne Spaulding**  
CSIS



**Samantha Ravich**  
Foundation for  
Defense of  
Democracies



**Tom Fanning**  
Southern Company



**Hon. Patrick Murphy**  
Fmr. Undersecretary,  
U.S. Army  
Fmr. U.S. Representative  
(D-PA)

## DATES

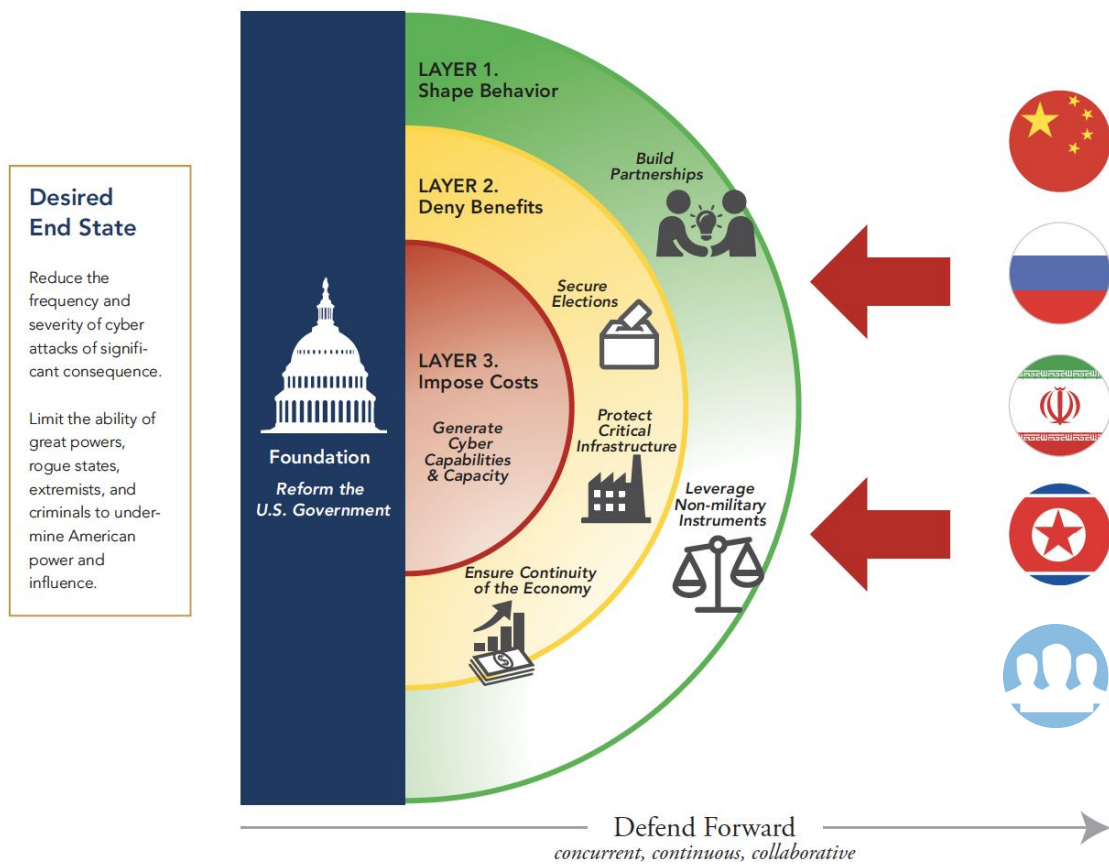
- **INITIAL MEETING**  
**APRIL 2019**
- **SOLARIUM EVENT**  
**OCTOBER 2019**
- **FINAL REPORT ISSUED**  
**11 MARCH 2020**



# A New Strategic Approach to Cybersecurity for the Nation



## Layered Cyber Deterrence



## The Implementation:

Pillar 1 - Reform the U.S. Government's Structure and Organization for Cyberspace;

Pillar 2 - Strengthen Norms and Non-Military Tools;

Pillar 3 - Promote National Resilience;

Pillar 4 - Reshape the Cyber Ecosystem towards Greater Security;

Pillar 5 - Operationalize Cybersecurity Collaboration with the Private Sector;

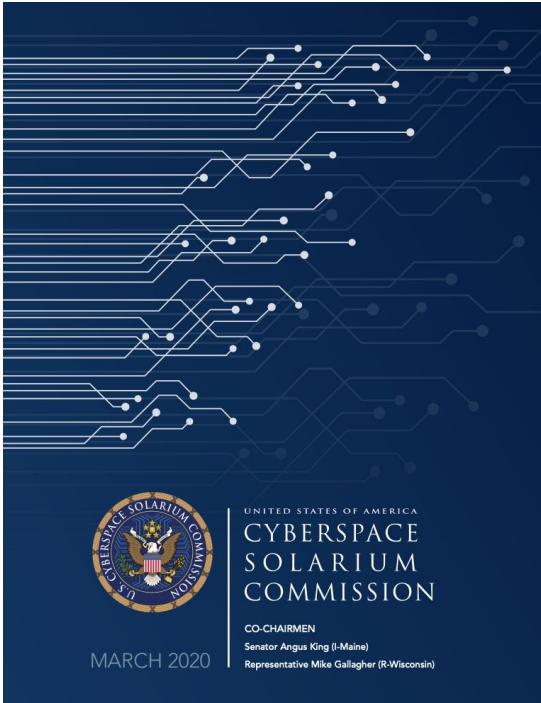
Pillar 6 - Preserve and Employ the Military Instrument of Power - and All Other Options to Deter Cyber-attacks at Any Level.

# Agenda



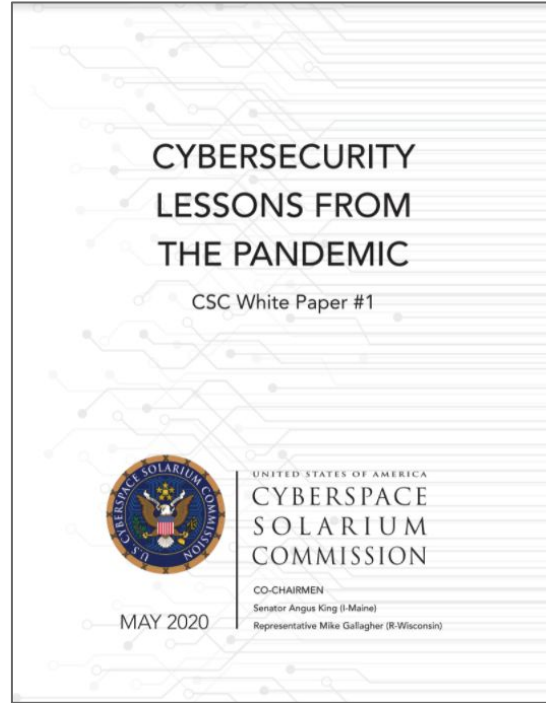
1. What is the Commission?
2. Content of:
  - a. Commission Report ← We are here
  - b. White Papers
3. Status
  - a. What happened in 2020?
  - b. What's the plan for 2021?
4. What this means for Resilience and Engaging the Private Sector

# Cyberspace Solarium Commission Publications

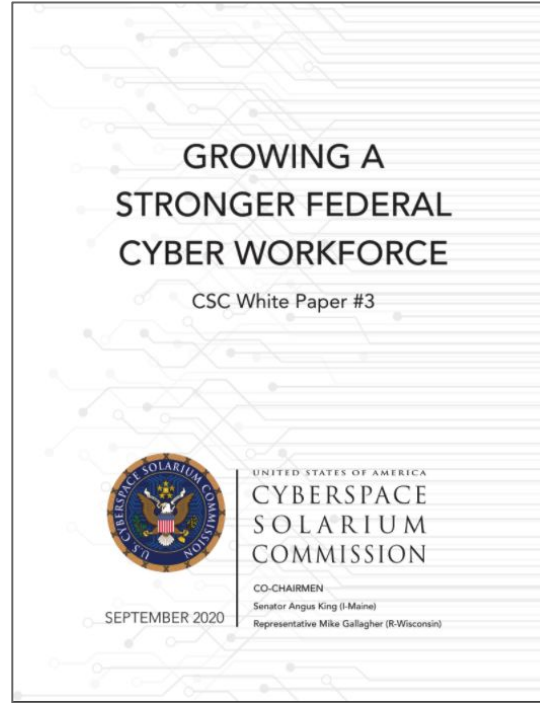


## Full Report:

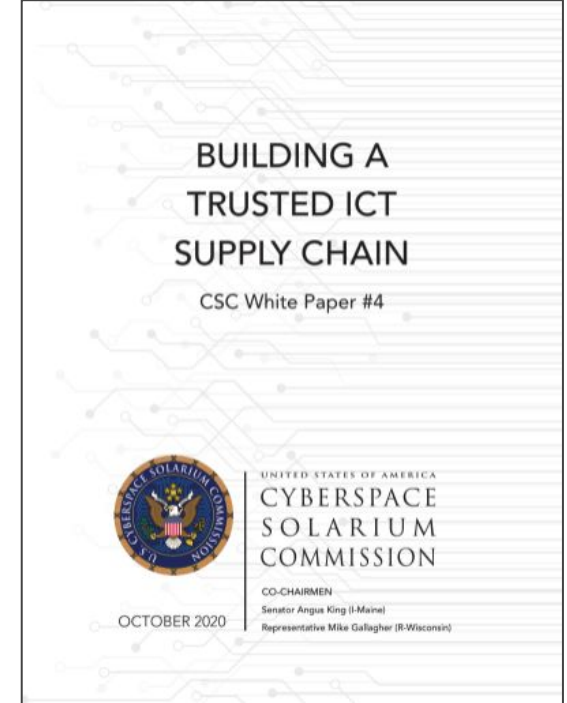
- 82 recommendations across many topics, including workforce development.
- Presented during April NICE WG call.



## White Paper: Cybersecurity Lessons from the Pandemic



## White Paper: Growing a Stronger Federal Cyber Workforce



## White Paper: Building a Trusted ICT Supply Chain

Available for download at [www.solarium.gov](http://www.solarium.gov)

# Pillar 1 - Reform the U.S. Government's Structure and Organization for Cyberspace



- Issue an **updated national cyber strategy** that emphasizes layered cyber deterrence, public-private collaboration, resilience, and defending forward.
- Create **House Permanent Select and Senate Select Committees on Cybersecurity** to streamline congressional oversight and authority.
- Establish a senate-confirmed **National Cyber Director** to lead national-level coordination for cyber strategy and policy.
- **Strengthen CISA** to ensure the national resilience of critical infrastructure and the cyber ecosystem.
- Recruit, develop, and retain a **stronger federal cyber workforce** to close the 33,000 worker shortfall and effectively implement many of the objectives laid out in this report.



## Pillar 2 - Strengthen Norms and Non-military Tools



- **Resourcing a new Bureau within the State Department led by an Assistant Secretary of State** to build a coalition.
- Strengthening our collaboration with **international law enforcement** partners.
- Engaging more actively in international technology **standards bodies** to ensure the internet and technology of the future shares our values and meets our expectations for security.
- **Building capacity** around the world to enable partners to share the burden of combating cyber threats.
- **Improving Attribution** of malign cyber activity to hold our adversaries accountable.
- **Reinvigorating cyber confidence-building measures (CBMs)** to increase global stability.



## Pillar 3 - Promote National Resilience



- Improve our capacity to **understand, assess, and manage national risk** - by:
  - resourcing and codifying the responsibilities of the various agencies within government, **sector risk management agencies** (sector-specific agencies) that manage day-to-day engagement with the private sector; and
  - tasking them, in coordination with DHS, to establish a **five-year national risk management cycle** and **critical infrastructure resilience strategy**. With this plan, we can create a fuller picture of risk and prioritize our resources and assets accordingly.
- Ensure we have the national capacity to **respond to and recover** from a significant cyber incident.
  - this means developing a **continuity of the economy (COTE)** plan to ensure the continuous operation of critical functions of the economy in the event of a significant cyber disruption; and
  - strengthening the U.S. government's ability to assist the private sector when a significant cyber incident occurs, through a **“cyber state of distress”** and a **“cyber response and recovery fund”**.
- Ensure the **security of our elections** and the resilience of our democracy, improving the funding and structure of the **Election Assistance Commission** and expanding **digital literacy efforts**.

# Pillar 4 - Reshape the Cyber Ecosystem towards Greater Security



- Improve the **security of technology** with:
  - **National Cybersecurity Certification and Labeling Authority**
  - **Hardware and software liability**
- Improve the **security behavior of users and organizations** by:
  - **Bureau of Cyber Statistics;**
  - **Reinvigorating the cybersecurity insurance market**
- Leverage **entities and organizations who can scale security** across the ecosystem:
  - **Cloud security certification** that providers can voluntarily attest to,
  - Incentivizing uptake of cloud services for **state and local governments and small and medium sized business**, and
  - working with major internet providers to ensure that **core internet protocols** are more secure.
- Manage the risk of increasingly complex and global technology **supply chains** by identifying, assessing, and filling gaps in our ICT dependencies through the **development and operationalization of an ICT-Industrial base strategy**.
- Promote **systemic data security** by **codifying a national data security and privacy protection law** to ensure the safe and appropriate handling of personal data.

# Pillar 5 - Operationalize Cybersecurity Collaboration with the Private Sector



- **Enhance government support to private-sector operations** by bringing to bear the government's unique authorities, resources, and intelligence capabilities by:
  - Codifying a new social contract between government and **systemically important critical infrastructure** to recognize the unique resources, roles, and responsibilities that are necessary to protect critical systems and assets.
  - Creating a formal process to **identify private-sector cybersecurity intelligence needs and priorities** to enhance their cybersecurity operations.
- **Improve combined situational awareness of cyber threats** to better support the U.S. government and private-sector cyber defensive efforts by:
  - Creating a single, **joint collaborative environment** to serve as the focal point for the sharing and fusing of all federal and critical infrastructure cyber threat information, insight, and other relevant data.
- Bolster the U.S. government's capacity to better coordinate its own cyber defense planning and operations and **integrate the government's operations with the private sector** by:
  - **resourcing and supporting an integrated cyber center within CISA** to act as the venue for public-private collaboration and the central coordinating body among federal cyber centers and private-sector partners; and
  - **Establishing a joint cyber planning office at CISA** to coordinate cybersecurity planning and readiness across the federal government and between public and private partners.

# Pillar 6 - Preserve and Employ the Military Instrument of Power & All Other Options to Deter Cyber Attacks at Any Level



- **Grow the capacity of the Cyber Mission Force (CMF)** to meet the current threat and growing mission requirements by:
  - Conducting a **force structure assessment of the CMF** in light of growing mission requirements and expectations, including an assessment of the NSA in its combat support agency role.
  - Creating a **Major Force Program (MFP) funding category** for U.S. Cyber Command to enhance funding flexibility
  - Reviewing the **delegation of authorities for cyber operations** to enable a more streamlined decision-making process, and flexible and rapid maneuver. This should include authorities granted to information operations.
  - Establishing a **Military Cyber Reserve** to play a central role in mobilizing a surge capacity during a cyber crisis and aid in talent management.
- **Ensure the security and resilience of critical conventional and nuclear weapons systems and functions** by:
  - Conducting a **vulnerability assessment of all segments of the nuclear command, control, and communications (NC3) enterprise** for mission and quality assurance.
  - Reporting annually to Congress on the **status of ongoing cyber vulnerability assessments of major weapons systems**. This should include assessments of legacy platforms and cyber vulnerabilities across networked systems.
  - Requiring **Defense Industrial Base (DIB) participation in a threat intelligence sharing program** to proactively and comprehensively address cyber threats and vulnerabilities to this sector.
  - Designating **threat hunting capabilities** on DIB networks and across the Department of Defense's Information Network to improve detection and mitigation of adversary cyber threats.

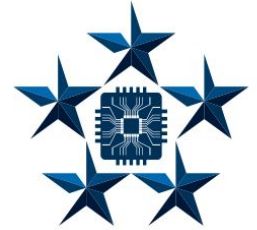


# Agenda



1. **What is the Commission?**
2. **Content of:**
  - a. **Commission Report**
  - b. **White Papers** ← **We are here**
3. **Status**
  - a. **What happened in 2020?**
  - b. **What's the plan for 2021?**
4. **What this means for Resilience and Engaging the Private Sector**

# Cybersecurity Lessons from the Pandemic



## Cybersecurity Challenges During a Pandemic

- Digitization of critical services
- The work-from-home economy
- Combatting opportunistic cybercrime

## What a Pandemic Can Teach us about Preparing for a Major Cyber Disruption

- Leadership and coordination processes
- Preparedness
- Prevention and mitigation
- Response and recovery
- Countering disinformation

# Growing a Stronger Federal Cyber Workforce



## Element of a Strategy

## Examples

### Organize

- Properly Identify and Utilize Cyber-Specific Occupational Classifications
- Build a Federal Cyber Service
- Establish Leadership and Coordination Structures

### Recruit

- Expand CyberCorps: Scholarship for Service
- Build on Centers of Academic Excellence
- Evaluate and Expedite the Personnel Security Clearance Process

### Develop

- Develop Apprenticeships
- Support Upskilling

### Retain

- Increase Pay Flexibility
- Develop Career Pathways
- Establish Rotational Programs and Talent Exchanges
- Address Systemic Inequities

### Stimulate Growth

#### Expand the Cyber Workforce Nationwide

- Coordinate U.S. Government Efforts
- Invest in Diversity, Equity, and Inclusion
- Incentivize Empirical Research
- Support Cyber Education
- Build the Military Workforce


# White Paper: Building a Trusted ICT Supply Chain



- To address these challenges, the Commission proposes a five-pillar strategy *built on the firm foundation of public-private and international partnerships*. Specifically, the Commission provides a roadmap and recommendations focused on:
  - *Identifying key technologies and equipment* through government reviews and public-private partnerships to identify risk.
  - *Ensuring minimum viable manufacturing capacity* through both strategic investment and the creation of economic clusters.
  - *Protecting supply chains from compromise* through better intelligence, information sharing, and product testing.
  - *Stimulating a domestic market* through targeted infrastructure investment and ensuring the ability of firms to offer products in the United States similar to those offered in foreign markets.
  - *Ensuring global competitiveness* of trusted supply chains, including American and partner companies, in the face of Chinese anti-competitive behavior in global markets.

# Agenda



1. **What is the Commission?**
2. **Content of:**
  - a. **Commission Report**
  - b. **White Papers**
3. **Status**  **We are here**
  - a. **What happened in 2020?**
  - b. **What's the plan for 2021?**
4. **What this means for Resilience and Engaging the Private Sector**



# What Happened in 2020?



## NDAA for FY21

- 27 Solarium Provisions
- Veto Overridden January 1, 2021
- Highlights:
  - National Cyber Director
  - Continuity of the Economy
  - Sector Risk Management Agencies
  - Force Structure Assessment of CMF
  - Assessment of DIB

116th Congress )	HOUSE OF REPRESENTATIVES	{ Report
2d Session )		{ 116-617

---

WILLIAM M. (MAC) THORBERRY  
NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2021

-----

CONFERENCE REPORT

to accompany

H.R. 6395

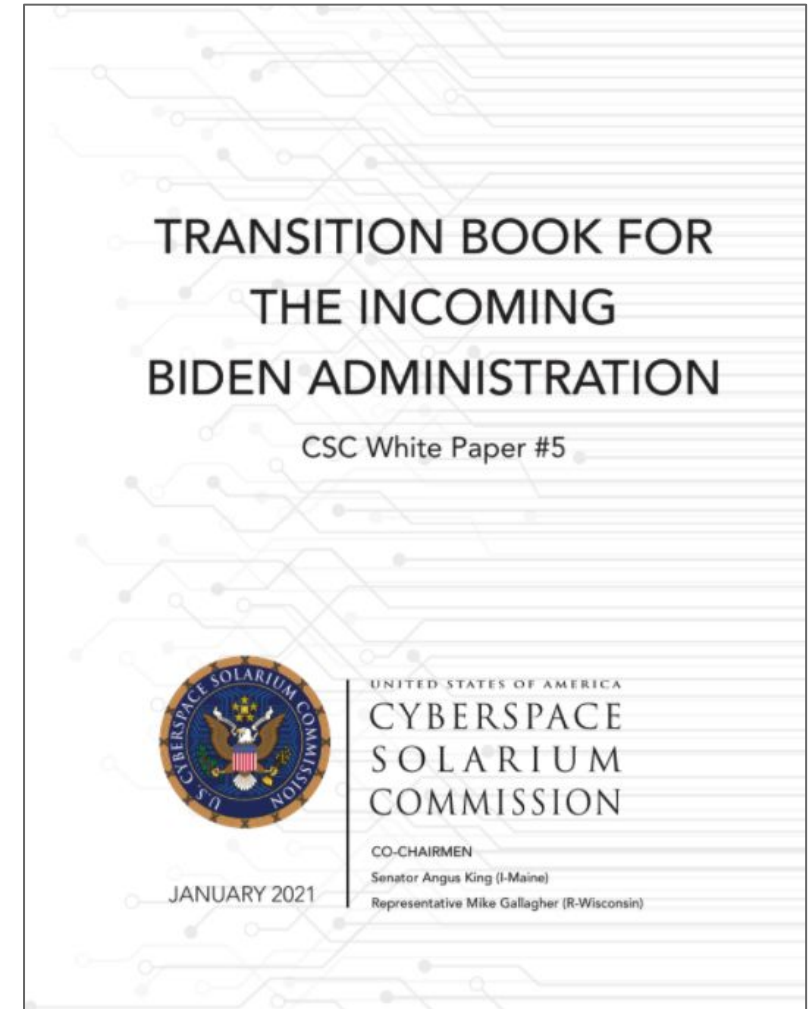
December 3, 2020.--Ordered to be printed

WILLIAM M. (MAC) THORBERRY NATIONAL DEFENSE AUTHORIZATION ACT  
FOR FISCAL YEAR 2021

# What is Coming in 2021?



- Executive:
  - Implement NCD
  - Issue Cyber Strategy
- Legislative Priorities:
  - Cyber Diplomacy Act
  - Supply Chain Legislation
  - Cyber Crime Victim Assistance
  - Workforce Provisions



# Agenda



1. **What is the Commission?**
2. **Content of:**
  - a. **Commission Report**
  - b. **White Papers**
3. **Status**
  - a. **What happened in 2020?**
  - b. **What's the plan for 2021?**
4. **What this means for Resilience and Engaging the Private Sector**

We are  
here



# Private Sector Engagement

